Department of Homeland Security Daily Open Source Infrastructure Report for 29 March 2007

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Department of Energy announced Wednesday two new Funding Opportunity Announcements, valued up to $14 million to better integrate the United States' universities into DOE's nuclear research and development programs; and contribute to assuring a new generation of engineers and scientists necessary for pursuing nuclear power. (See item 1)
- The Department of Justice has announced that a Bulgarian member of a transnational criminal group has been arrested on U.S. charges by law enforcement authorities in Budapest, Hungary, in connection with an elaborate Internet scheme responsible for defrauding American citizens of over $350,000. (See item 11)
- The U.S. Department of Homeland Security announced Tuesday the award of $34.6 million in equipment and training to first responders across the nation as a part of the fiscal year 2006 Commercial Equipment Direct Assistance Program. (See item 29)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 28, Department of Energy* — **Department of Energy issues $14 million in funding opportunity announcements to U.S. universities for nuclear research.** The Department of

Energy (DOE) Wednesday, March 28, announced two new Funding Opportunity Announcements (FOA), valued up to $14 million to better integrate the United States' universities into DOE's nuclear research and development programs; and contribute to assuring a new generation of engineers and scientists necessary for pursuing nuclear power. These FOAs support the Global Nuclear Energy Partnership (GNEP) University Readiness and the Nuclear Energy Research Initiative for Consortia (NERI−C). These new awards will bring total Fiscal Year 2007 funding to universities that support nuclear energy programs to over $54 million. For additional information on this announcement, GNEP and nuclear R&D programs, visit: http://www.nuclear.gov/.
Source: http://www.energy.gov/news/4901.htm

2. *March 28, Platts Energy Bulletin* — **EIA to begin monthly ethanol, biofuel surveys.** The Energy Information Administration (EIA) plans this year to begin development of monthly ethanol and biofuels data surveys to reflect the growing importance of the fuels in the market, EIA administrator Guy Caruso said Wednesday, March 28. EIA is also planning a redesign of "key oil and gas surveys" to capture evolving market conditions, Caruso said at an EIA energy modeling conference.
Source: http://www.platts.com/Oil/News/6370257.xml?sub=Oil&p=Oil/New s

3. *March 28, Platts Energy Bulletin* — **European Commission energy chief welcomes EU−U.S. energy cooperation.** EU energy commissioner Andris Pieblags Tuesday, March 27, welcomed increased cooperation in the field of energy supply and security between the European Union and U.S. and offered the U.S. support in the field of energy efficiency. Speaking after a meeting in Washington with U.S. energy secretary Samuel Bodman, Piebalgs said he was pleased with progress made since an EU−U.S. declaration June 2006 to increase strategic energy cooperation, particularly in research on biofuels development and energy efficiency. But Piebalgs said new technologies were only "part of the picture." "The efficient use of energy is also a key element and I believe that in this sphere the EU has a lot to offer in terms of know−how and best practice", Piebalgs said. "Bilateral cooperation has been strengthened notably on biofuels, clean coal and carbon sequestration, energy efficiency, methane recovery, and, more generally, on energy security issues," in the past year, the European Commission said.
Source: http://www.platts.com/Electric%20Power/News/8959647.xml?sub= Electric%20Power&p=Electric%20Power/News

4. *March 28, Independent (UK)* — **Sicily to build world's first solar power plant.** The world's first solar power plant, which will yoke the power of the sun with gas, will go on stream on the sunny east coast of Sicily by 2009, if a deal signed by the Italian government this week goes according to plan. The project is named Archimedes. The existing gas−fired power plant on the site will be augmented by Archimedes, which should produce five megawatts of electricity, enough for 4,500 families. Archimedes' trump card is the fact that it will produce solar energy 24 hours a day, not just when the sun is shining. The plant's battery of parabolic mirrors will focus the sun's rays on pipes, through which runs a saline liquid that can store heat and retain it for hours.
Source: http://news.independent.co.uk/europe/article2398895.ece

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *March 28, Associated Press* — **Tennessee chemical fire forces evacuations.** Fire broke out in a chemical storage facility Wednesday, March 28, in Humboldt, TN, forcing as many 700 people to evacuate homes and businesses in the area. Homes downwind from the fire were evacuated because of the smoke, and workers at nearby manufacturing plants were told to leave as a precaution, Mayor Allen Barker said. The fire was at the Helena Chemical Co. warehouse and office in Humboldt, a West Tennessee town of about 9,500 residents 15 miles northwest of Jackson.
   Source: http://hosted.ap.org/dynamic/stories/C/CHEMICAL_FIRE?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT

[Return to top]

Defense Industrial Base Sector

6. *April 01, National Defense* — **Defense seeking $131M for energy−saving projects.** The Pentagon has asked Congress for $131 million to develop energy−saving technologies during the next five years. The proposed budget would fund a mix of fuel cells, generators and engine technologies. The projects were selected based on input from the military services, says John Young, director of defense research and engineering. His office oversees the so−called “Energy Security Task Force,” which was created to find ways to reduce fossil−fuel consumption. The Department of Defense is the largest single consumer of fuel in the United States even though it accounts for just 1.2 percent of the nation’s energy use. Nearly 60 percent of the Pentagon’s energy consumption is in the form of jet fuel, which powers not only aircraft, but also tanks and some Navy ships.
   Source: http://www.nationaldefensemagazine.org/issues/2007/April/Def enseSeeking.htm

[Return to top]

Banking and Finance Sector

7. *March 28, Websense Security Labs* — **Multiple phishing alerts.** Websense Security Labs has received reports of phishing attacks that target Alhambra Credit Union, Bank of Hanover, and Weber Credit Union customers. Users receive a spoofed email message, which claims that if they take a survey to give feedback on the quality of services, they will get a $45 − $99 credit to their account. The emails provide a link to a phishing site that attempts to collect personal and account information.
   Source: http://www.websense.com/securitylabs/alerts/

8. *March 28, Department of the Treasury* — **Treasury takes action against major Medellin−based trafficker and his financial empire.** The Department of the Treasury's Office of Foreign Assets Control (OFAC), on Wednesday, March 28, named Fabio Enrique Ochoa Vasco (a.k.a."Carlos Mario"), a major Medellin−based drug trafficker, as a principal individual on its list of Specially Designated Narcotics Traffickers (SDNTs). At the same time, OFAC

designated 45 companies and 64 individuals in Ochoa Vasco's extensive criminal and financial network, across Colombia, Belize, Ecuador, Guatemala, Honduras, Jamaica, Mexico, and Panama. Fabio Enrique Ochoa Vasco is the head of one of the most powerful Medellin−based drug trafficking organizations today," said OFAC Director Adam J. Szubin. Wednesday's designation action freezes any assets the designees may have subject to U.S. jurisdiction, and prohibits all financial and commercial transactions by any U.S. person with the designated companies and individuals. This is OFAC's first designation of a significant narcotics trafficker operating out of Medellin, Colombia since the issuance of Executive Order 12978 in October 1995. Fabio Enrique Ochoa Vasco has been involved in narcotics trafficking activities from Colombia to the United States since at least 1981.
Source: http://www.treasury.gov/press/releases/hp330.htm

9. *March 27, Government Accountability Office* — **GAO−07−256: Information Security: Sustained Progress Needed to Strengthen Controls at the Securities and Exchange Commission (Report).** In carrying out its mission to ensure that securities markets are fair, orderly, and efficiently maintained, the Securities and Exchange Commission (SEC) relies extensively on computerized systems. As part of its audit of SEC's financial statements, the Government Accountability Office (GAO) assessed (1) SEC's actions to correct previously reported information security weaknesses and (2) the effectiveness of controls for ensuring the confidentiality, integrity, and availability of SEC's information systems and information. SEC has made important progress toward correcting previously reported information security control weaknesses. Specifically, it has corrected or mitigated 58 of the 71 weaknesses previously reported as unresolved at the conclusion of GAO's 2005 audit. GAO recommends that the SEC Chairman improve the implementation of its policies and procedures, control tests and evaluations, and remedial action plans as part of its agencywide information security program. In commenting on a draft of this report, SEC stated that it will actively work to implement GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d07256high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−256

10. *March 27, InformationWeek* — **UK: Stolen laptops hold information on 11,500 children.** Three laptops containing personal information on 11,500 children were stolen earlier this month from a National Health Services office in the United Kingdom and police are worried the information may fall into the wrong hands. The computers were taken from Primary Care Trust office on the afternoon of Wednesday, March 21, according to an advisory from the Nottinghamshire County NHS. The laptops contained the names, addresses, and dates of birth of child patients between the ages of 8 months and 8 years old. "There was no health information or other details on the stolen computer," said Wendy Saviour, chief executive of the Nottinghamshire County NHS, in a written statement. "The information was protected by a password. We have, however, written to all the 9,742 families affected by this theft to inform them of what has happened."
Source: http://www.informationweek.com/news/showArticle.jhtml;jsessionid=OPPYC2DLYKVF2QSNDLPCKHSCJUNN2JVN?articleID=198700506

11. *March 26, Department of Justice* — **Bulgarian woman arrested and charged with conspiracy and money laundering.** A Bulgarian member of a transnational criminal group has been arrested on U.S. charges by law enforcement authorities in Budapest, Hungary, in

connection with an elaborate Internet scheme responsible for defrauding American citizens of over $350,000. On March 1, 2007, a federal grand jury in the District of Columbia returned an indictment charging Mariyana Feliksova Lozanova with conspiracy to commit wire fraud and conspiracy to commit money laundering. According to the indictment, from March to April 2006, Lozanova and others allegedly participated in a scheme to advertise merchandise for sale on the eBay Website, including expensive motor vehicles and boats. When the U.S. victims expressed interest in the merchandise, they were contacted directly by an email from a purported seller. The victims were then instructed to wire transfer payments through "eBay Secure Traders"—an entity which has no actual affiliation to eBay but was used as a ruse to persuade the victims that they were sending money into a secure escrow account pending delivery and inspection of their purchases. Instead, the victims' funds were allegedly wired directly into one of several bank accounts in Hungary or Slovakia controlled by Lozanova and her co−conspirators.
Source: http://washingtondc.fbi.gov/dojpressrel/pressrel07/wfo032607 .htm

[Return to top]

Transportation and Border Security Sector

12. *March 28, Reuters* — **Canada's Harmony Airways to end scheduled service.** Harmony Airways, a five−year−old Canadian full−service airline, said Tuesday, March 27, it will end scheduled flights next month, blaming rising costs and competition from larger rivals. The privately held carrier said it will lay off 350 workers. It will not seek protection from creditors and might try to reorganize itself into a charter service, however. It is the latest of several Canadian start−up airlines to be grounded in recent years in a sector dominated by Air Canada and WestJet Airlines.
Source: http://www.usatoday.com/travel/flights/2007−03−28−canadian−airline−to−halt−scheduled−service_N.htm

13. *March 28, Government Accountability Office* — **GAO−07−412: Port Risk Management: Additional Federal Guidance Would Aid Ports in Disaster Planning and Recovery.** U.S ports are significant to the U.S. economy, handling more than 2 billion tons of domestic and import/export cargo annually. Since September 11, 2001, much of the national focus on ports' preparedness has been on preventing potential acts of terror, the 2005 hurricane season renewed focus on how to protect ports from a diversity of threats, including natural disasters. This report was prepared under the authority of the Comptroller General to examine (1) challenges port authorities have experienced as a result of recent natural disasters, (2) efforts under way to address these challenges, and (3) the manner in which port authorities plan for natural disasters. The Government Accountability Office (GAO) reviewed documents and interviewed various port stakeholders from 17 major U.S. ports. To ensure that ports achieve adequate planning for natural disasters, GAO recommends that the Secretary of Homeland Security encourage port stakeholders to use existing forums for discussing all−hazards planning.
Highlights: http://www.gao.gov/highlights/d07412high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−412

14. *March 28, Government Accountability Office* — **GAO−07−617T: Airport Finance: Preliminary Analysis Indicates Proposed Changes in the Airport Improvement Program**

May Not Resolve Funding Needs for Smaller Airports (Testimony). To address the strain on the aviation system, the Federal Aviation Administration (FAA) has proposed transitioning to the Next Generation Air Transportation System. To finance this system and to make its costs to users more equitable, the administration has proposed fundamental changes in the way that FAA is financed. As part of the reauthorization, the administration proposes major changes in the way that grants through the Airport Improvement Program are funded and allocated to the 3,400 airports in the national airport system. In response, the Government Accountability Office (GAO) was asked for an update on current funding levels for airport development and the sufficiency of those levels to meet planned development costs. This testimony comprises capital development estimates made by FAA and Airports Council International, the chief industry association; analyzes how much airports have received for capital development and whether this is sufficient to meet future planned development; and summarizes the effects of proposed changes in funding for airport development. This testimony is based on ongoing GAO work. Airport funding and planned development data are drawn from the best available sources and have been assessed for their reliability.
Highlights: http://www.gao.gov/highlights/d07617thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−617T

15. *March 27, Aero−News* — **FAA calls for GPS runway mapping system.** Knowing where you are on what runway or taxiway is critical information −− especially if unfamiliar with an airport, in poor weather, or at night. Traditionally, pilots have acquired that information by simply looking out their windshield. Now, the Federal Aviation Administration (FAA) wants to provide a moving map display that uses Global Positioning System (GPS) as an adjunct to the electronic flight bag. After reviewing safety data, the FAA announced they are changing their certification process to enable this technology to be available later this year while maintaining all appropriate safety standards.
Source: http://www.aero−news.net/index.cfm?ContentBlockID=8129a5b0−2b09−48e1−af0d−37f0d7d38b4f&

16. *March 27, USA TODAY* — **TSA boosts checks on airport workers.** The Transportation Security Administration (TSA) is stepping up screening of airport workers nationwide amid growing concern that nearly 1 million employees can get into airplanes or other restricted areas without going through security. Teams of screeners, air marshals, and inspectors will go from airport to airport, spending several days at a time searching workers and checking airplane cabins, agency chief Kip Hawley told USA TODAY. The strategy, dubbed "surge," comes three weeks after two Orlando−based airline workers were charged with carrying 14 guns onto a Comair flight. Their arrests heightened calls in Congress for workers to be screened like airline passengers. The TSA has required more airport workers to pass background checks and last year started randomly screening the workers. In its first "surge," the agency sent 160 security officers to five airports in south Florida and Puerto Rico for several days after the Comair employees were arrested. Hawley said the extra TSA workers will "really be noticeable" to deter potential terrorists.
Source: http://www.usatoday.com/travel/flights/2007−03−27−tsa−airpor t−workers_N.htm

17. *March 23, Associated Press* — **Airlines question rules for icy takeoffs.** During a late−winter storm recently, hundreds of passengers remained aboard grounded jets at New York's John F. Kennedy International Airport for as long as 14 hours as deicing operations ground to a halt.

Furious travelers castigated the airlines for not letting them disembark sooner. The Federal Aviation Administration (FAA) and the airlines have been at odds for two years about the protocols for taking off in storms that produce light ice pellets, a term for the stinging sleet that occurs when snow melts, then refreezes, as it falls from the sky. The dispute began in October 2005 when the FAA temporarily barred flights in ice pellets after a Canadian study indicated that anti−icing fluids might not be as effective against the sticky granules as previously thought. Air carriers protested and the FAA in August began allowing flights again, but only if a takeoff is accomplished within 25 minutes of a deicing procedure. Planes that don't beat that deadline have to be deiced again, creating headaches for airlines because departing flights routinely exceed the 25−minute threshold at major airports.
Source: http://www.usatoday.com/travel/flights/2007−03−23−icy−takeof f−rules_N.htm

[Return to top]

Postal and Shipping Sector

18. *March 27, DM News* — **Communication is key in new postal environment: Potter.** Dialog between mailers and the U.S. Postal Service is key if the mailing industry is going to successfully navigate new roads that have barely been mapped. This was a key message from Postmaster General John E. Potter in his keynote address at the National Postal Forum Monday, March 26. Mr. Potter was referring to the new postal law that took effect on December 20 that changes the role of the agency and the Postal Regulatory Commission (PRC). Under the law, the PRC must write a new set of rules on how to establish mail rates; ensure compliance with the new rules; act on complaints about postal rates and poor mail delivery; review whether mail delivery is meeting the needs of the nation; and, if necessary, use subpoena power to get information from the Postal Service. Mr. Potter also discussed how mailers and the USPS have to work together to mitigate some of the larger rate increases that they face. Rate increases go into effect May 14 for most mailers.
Source: http://www.dmnews.com/cms/dm−news/direct−mail/40527.html

19. *March 27, DM News* — **UPS announces automated interception service.** United Parcel Service (UPS) has launched UPS Delivery Intercept, an automated service that enables shippers to intercept and reroute packages before they're delivered. Atlanta−based UPS said the service is the industry's only Web−enabled package interception service. Shippers can access the service at any time to request UPS to intercept packages being shipped from and to anywhere in the United States and Puerto Rico. UPS Delivery Intercept is powered by UPS's package flow technology, which enables UPS not only to map more efficient routes for drivers but also to flag packages for special handling while they are in the UPS network. Interceptions can be executed after a package is already on board a delivery vehicle. Shippers have a number of options once UPS intercepts a package, including return the package to the shipper redirect the package to a new address; hold the package for delivery on a future date; or hold the package for pickup by the consignee.
Source: http://www.dmnews.com/cms/dm−news/direct−mail/40530.html

[Return to top]

Agriculture Sector

20. *March 28, Yakima Herald−Republic (WA)* — **New extension service lab helps rapidly identify pests, disease.** It's called a seed bug, a specimen of which landed on Mike Bush's desk at Yakima County, WA's Cooperative Extension Service in the county courthouse. An extension Master Gardener had passed it on for Bush, an entomologist and tree fruit extension agent, to identify. He may have an answer soon −− as in a day or so. The quick turnaround is the essence of a pest−and−disease identification network that now stretches throughout the state and the West. Extension agents, pathologists, entomologists and weed scientists are using digital images sent for identification. Bush said the old system of mailing specimens took two weeks or longer. The Distance Diagnostics Through Digital Imaging Network is funded by a Department of Homeland Security grant to quickly detect threats to agriculture. Norman Dart, extension coordinator for the network based at the Western Washington Research and Extension Center in Puyallup, said the project had its origins to combat biological terrorism. But it has taken on a broader approach to create a system to watch for disease−causing organisms.
Source: http://www.yakima−herald.com/page/dis/288522109293836

21. *March 26, Associated Press* — **Navajo Nation watches ID tracking technology take hold.** Navajo cattle and sheep ranchers are being required to put radio identification tags on their animals. They attach to an animal's ear and can hold information about the age, vaccinations, nutrition and health of the animal. A plastic wand can scan the tag and match it to information stored in a computer. The radio tags are among regulations for livestock and other animals adopted with the Navajo Nation Council in May 2006.
Source: http://www.kold.com/Global/story.asp?S=6278662

[Return to top]

Food Sector

22. *March 27, Food Production Daily* — **Steam cleaning cuts salmonella in meat.** Using commercial household stream cleaning can provide smaller processing plants with a low cost method of decontaminating beef and hog carcasses, according to a recent study. Commercial household steam cleaning can be an effective and economical method of reducing naturally occurring bacteria on freshly slaughtered beef and hog carcasses, according to scientists at the University of Georgia. Tests were conducted on 72 beef and 72 hog carcasses from four small or very small processing plants. Three sites on one side of each carcass were exposed to 60 seconds of steam treatment, while the other side remained untreated. Samples were taken before, immediately after and 24 hours following the steam treatment. Prior to treatment, salmonella was found in five of the carcasses, but all tested negative for the pathogen after steam exposure. Aerobes, coliforms, and enterobacteriaceae at the three anatomical locations on both types of carcasses reduced following steam treatment. Aerobes are bacteria and high levels can indicate possible contamination, while coliforms are a common bacterial indicator of sanitary quality of food and water as they are found in animal feces. Enterobacteriaceae is the family of bacteria that includes salmonella and Escherichia coli (E.coli).
Source: http://www.foodproductiondaily.com/news/ng.asp?n=75270−salmo

nella−steam−contamination

[Return to top]

Water Sector

23. *March 27, NBC 4 (DC)* — **Residents report ammonia in water.** Somehow ammonia got into the water in Reston, VA, and officials said it has gotten into people's eyes when they shower. Initial reports said one child and two adults in the Fairfax area have had stinging in their eyes after taking showers. The Fairfax County Fire and Rescue Department issued a statement Monday, March 26, saying that they were aware of the ammonia smell and taste in the water. Officials said the situation is a result of repair work conducted earlier in the afternoon at the Potomac Water Treatment Facility. The situation, which caused the odor, has been corrected, and Fairfax County fire crews flushed the system.
Source: http://www.nbc4.com/news/11391121/detail.html

[Return to top]

Public Health Sector

24. *March 28, Reuters* — **Indonesia confirms bird flu deaths.** Indonesia announced three deaths from bird flu on Wednesday, March 28, taking its overall human toll from the virus to 69 fatalities. The virus is endemic among fowl in many parts of Indonesia, the world's fourth most populous country. Human cases generally involve contact with infected birds. A health ministry official said on Wednesday second tests had confirmed a teenager, a 22−year−old woman and a 39−year−old man had died from bird flu in Indonesia. The 39−year−old man among the three was from East Java and "on March 11 his and neighbors' chickens died suddenly. The tests showed that they were infected by avian flu," Muhammad Nadirin at the health ministry's bird flu center told Reuters.
Source: http://www.reuters.com/article/worldNews/idUSJAK732242007032 8

25. *March 27, Agence France−Presse* — **Two children diagnosed with bird flu in Egypt.** Two Egyptian children have been infected with avian flu, the health ministry announced on Tuesday, March 27, bringing to 29 the number of infections reported since the virus appeared in the country a year ago. Rihab Mahmud Helmi, a six−year−old girl, and Mahmud Gomaa Mohammed, a five−year−old boy, have been brought to Cairo for treatment, ministry spokesman Abdel Rahman Shaheen said. The children −− from separate southern Egyptian cities −− are in stable condition and being treated with the Tamiflu drug. Their families are under observation. The announcement comes only two days after another child, three−year−old Hagar Mohammed Awadallah from the southern city of Aswan, was diagnosed with the H5N1 strain of the virus.
Source: http://news.yahoo.com/s/afp/20070327/hl_afp/healthfluegypt_070327155418;_ylt=AhJupcddlZ4SlLSnTiXwe9mJOrgF

26. *March 23, Charleston Daily Mail (WV)* — **Hantavirus may have killed one man, infected another.** Local health officials want to know whether the rodent−born Hantavirus killed a

Belle, WV, man and infected another resident. Lab results from local hospitals indicated that both men were infected with Hantavirus, said Kerry Gateley, director of the Kanawha−Charleston Health Department. Blood samples have been sent to the U.S. Centers for Disease Control and Prevention for additional testing. Health department workers have interviewed friends and family members of the men, and visited their homes and work sites. One of the Belle men died about seven weeks ago. The lab result on the other man indicated an "old Hantavirus infection," Gateley said. The man was never hospitalized. "It came back that some time in the past, the person could have been exposed to Hantavirus," Gateley said.
Hantavirus information: http://www.cdc.gov/ncidod/diseases/hanta/hps/index.htm
Source: http://www.dailymail.com/story/News/+/2007032314/Hantavirus−may−have−killed−one−man−infected−another

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

27. *March 28, Trenton Times (NJ)* — **Trenton acts on emergency alert plan.** When an emergency arises that merits mass notification of city residents, every household in Trenton, NJ, will receive a phone call or e−mail from Mayor Douglas H. Palmer. This is the future that Palmer painted for the city Tuesday, March 27, when he announced the launch of a rapid phone and e−mail system designed to alert city residents of emergency conditions. Whether it's the threat of a flood, a water−main break, a chemical spill or a gentle reminder to not put your garbage out on the curb during a holiday, Palmer's messages will reach you on your land line, by Internet, or cell phone. The rapid emergency response system, which is similar to reverse 9−1−1, is essential for Trenton because it's a city prone to flooding, Palmer said. Palmer said he hopes the system will aid city officials in preparing for potential bio−terror and pandemic flu outbreaks.
Source: http://www.nj.com/timesoftrenton/stories/index.ssf?/base/news−9/1175054775208990.xml&coll=5

28. *March 28, Government Accountability Office* — **GAO−07−193: Disaster Preparedness: Better Planning Would Improve OSHA's Efforts to Protect Workers' Safety and Health in Disasters.** Concerns about the safety and health of workers involved in the response to Hurricane Katrina included their exposure to contaminated floodwaters and injuries from working around debris. The Department of Labor’s Occupational Safety and Health Administration (OSHA) is responsible for coordinating federal efforts to protect the safety and health of workers involved in the response to large national disasters. Under the Comptroller General’s authority, the Government Accountability Office (GAO) initiated a number of Katrina−related reviews. For this review, GAO examined (1) what is known about the number of response and recovery workers deployed to the Gulf Coast in response to Hurricane Katrina; (2) the extent to which OSHA tracked injuries and illnesses sustained by these workers; and (3)

how well OSHA met the safety and health needs of workers. To address these issues, GAO reviewed reports; analyzed data; interviewed federal, state, and local officials; and conducted site visits. GAO is making recommendations to the Secretaries of Labor, Homeland Security, and Health and Human Services designed to improve OSHA's efforts during future disasters.
Highlights: http://www.gao.gov/highlights/d07193high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−193

29. *March 27, Department of Homeland Security* — **DHS provides first responders $34.6 million in equipment and training programs.** The U.S. Department of Homeland Security (DHS) announced Tuesday, March 27, the award of $34.6 million in equipment and training to first responders across the nation as a part of the fiscal year 2006 Commercial Equipment Direct Assistance Program (CEDAP). DHS awarded more than 2,000 direct assistance grants to ensure that law enforcement and emergency responders receive specialized equipment and training to meet their homeland security mission. "CEDAP is yet another mechanism for the department to work with our local homeland security partners in strengthening this nation's ability to prevent, protect, respond and recover from a natural disaster or terrorist attack," said George Foresman, Under Secretary for Preparedness. "This program enhances state and local communities' capabilities as well as arms their first responders with the tools to build stronger regional coordination." This program also focuses on smaller communities and metropolitan areas not eligible for the Urban Areas Security Initiative grant program. Awardees are required to receive training on their awarded equipment either on−site or at a CEDAP training conference.
Source: http://www.dhs.gov/xnews/releases/pr_1175027617227.shtm

30. *March 27, Associated Press* — **Report calls for improved emergency planning.** The Valentine's Day winter storm that left hundreds of motorists stranded for hours on several Pennsylvania interstate highways revealed "a remarkable lack of awareness and understanding" of the state's emergency management system, according to an independent report released Tuesday, March 27. The report cited an array of shortcomings in staffing, supervision, technology and communication in three state agencies −− the Pennsylvania Department of Transportation, the Pennsylvania Emergency Management Agency and the state police −− that compounded the problems caused by the storm. Governor Ed Rendell told a Capitol news conference that he has instructed the heads of those agencies to begin implementing the consultant's recommendation that emergency planning be given a higher priority.
Source: http://www.citizensvoice.com/site/news.cfm?newsid=18133032&BRD=2259&PAG=461&dept_id=455154&rfi=6

[Return to top]

Information Technology and Telecommunications Sector

31. *March 28, InformationWeek* — **Malware disrupts half of global businesses, study finds.** Malware is disrupting nearly half of worldwide businesses, a new study reports. The Webroot State of Internet Security study reports that out of 600 global businesses that were surveyed, 43% of them said they're suffering business disruptions due to malware and more than 60% do not have an information security plan. According to Webroot's quarterly study, more than 40% of the companies surveyed said spyware was causing business losses. Webroot's analysts noted in the study that most unsettling finding is that 26% of enterprises reported that confidential

information had been compromised as a result of spyware. Thirty−nine% reported Trojan attacks, 24% reported system monitor attacks, and 20% reported pharming and keylogger attacks. Webroot also reported that analysts there have found that 1.7% (or 4.2 million) of 250 million URLs around the world harbor malware. Almost 3 million of those malicious sites were discovered in 2006 alone.
Report: http://www.webroot.com/company/pressroom/pr/sois−07−q3.html
Source: http://www.informationweek.com/news/showArticle.jhtml;jsessionid=4UTCFJLHMBUBCQSNDLRSKHSCJUNN2JVN?articleID=198700793

32. *March 28, IDG News Service* — **AC failure temporarily shuts down Florida state computers.** Critical air conditioning service has been restored to a state government data center in Florida after crews scrambled to replace a failed chiller with a backup. At 5:15 p.m. EDT on Monday, March 26, a water leak was discovered in a chiller that cools a 1,200−server data center. That center provides computing power to a state Website, the office of the governor, the Department of Revenue and other state agencies in the capital of Tallahassee. Concerned that the air conditioning breakdown could overheat the data center and damage the equipment, state agencies were ordered to shut down their computer systems that evening, said DMS communications unit's James Miller. Two 400−ton capacity backup chillers were shipped from Orlando and Birmingham, AL, and service was restored to the data center by 2 a.m. EDT Tuesday, said Miller. The DMS has service−level agreements with state agencies requiring that computer systems be functioning at a certain level of reliability, but because the downtime was late at night, no SLAs were breached, Miller said.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014704&intsrc=hm_list

33. *March 28, SC Magazine* — **Cisco VoIP technology open to DoS attacks.** Cisco Systems said Wednesday, March 28, that its Unified CallManager and Presence Server software contain a number of vulnerabilities that could permit DoS attacks. CallManager versions 3.3, 4.1, 4.2 and 5.0, in addition to Presence Server version 1.0, are affected by the flaws. Currently there are no workarounds for the bugs, and the company is developing a permanent fix, which will be distributed when it becomes available, according to a Cisco advisory. In the meantime, users should filter traffic as described in the advisory. Andrew Storms, director of security operations for nCircle, said the flaws are relatively easy to exploit and can result in a loss of telephone service for an enterprise.
Cisco Advisory: http://www.cisco.com/en/US/products/products_security_advisory09186a008080f17b.shtml
Source: http://scmagazine.com/us/news/article/646876/cisco−voip−technology−open−dos−attacks/

34. *March 28, Secunia* — **IBM Lotus Domino script insertion and buffer overflows.** Some vulnerabilities have been reported in IBM Lotus Domino and Lotus Domino Web Access, which can be exploited by malicious people to conduct script insertion attacks, cause a DoS (Denial of Service), and potentially compromise a vulnerable system. 1) A boundary error within the IMAP service (nimap.exe) during CRAM−MD5 authentication can be exploited to cause a buffer overflow by passing an overly long username (more than 256 bytes); 2) An error in the LDAP service when handling certain requests can be exploited to cause a heap−based buffer overflow via a specially crafted request containing a string longer than 65535 bytes; 3)

Certain input in e−mail messages is not properly sanitised by Lotus Domino Web Access before being displayed. This can be exploited to insert arbitrary HTML and script code, which is executed in a user's browser session in context of an affected site when a malicious message is viewed. Users should upgrade to version 6.5.6 or 7.0.2 Fix Pack 1.
IBM Advisories: http://www−1.ibm.com/support/docview.wss?uid=swg21257028
http://www−1.ibm.com/support/docview.wss?uid=swg21257248
http://www−1.ibm.com/support/docview.wss?uid=swg21257026
Source: http://secunia.com/advisories/24633/

35. *March 27, Computerworld* — **Critical bugs in StarOffice, OpenOffice suites.** Bugs in Sun Microsystems Inc.'s StarOffice and OpenOffice.org's OpenOffice application suites allow attackers to snatch control of a computer by serving up malicious documents or URLs, the two organizations said Monday, March 26. The flaws are in StarOffice's StarCalc spreadsheet and in how the suite handles URLs, said Sun in two advisories posted to its Website. Neither vulnerability has been patched, and Sun had no workaround or temporary defense recommendations. Nor could Sun immediately provide a patch delivery date. The bugs were also acknowledged yesterday by OpenOffice.org, the open−source organization that produces the same−name free application suite that shares a code base with Sun's StarOffice. No fixes are available for current production versions of OpenOffice.org, but the latest release candidate (RC) of v.2.2 includes patches.
OpenOffice.org 2.2 RC4 can be downloaded here: http://www.openoffice.org/
Advisory from Sun Microsystems:
http://sunsolve.sun.com/search/document.do?assetkey=1−26−102 794−1
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014638&intsrc=hm_list

36. *March 27, IDG News Service* — **Web attacks get personal.** Malware purveyors are increasingly tailoring their virus distribution and attack techniques to take advantage of different classes of end−users, according to researchers with the Internet Security Systems' X−Force team at IBM. Cyber−criminals are creating malware outlets and code executions that scan readily−available details about people's' computing posture to find appropriate recipients for their work. The approach uses any information that is found to isolate the right attack to deliver based on factors like the particular Web browser or operating system that an individual who being targeted is using. Cyber−criminals are also loading malware−infected Web pages with numerous code execution threats to assault many different aspects of varied sets of users with dozens of pieces of code being served up on a single URL. Many of the threats are hidden in individual elements of Web pages, including flash files, pdfs and images, which may each contain multiple attacks meant to take advantage of different vulnerabilities.
Source: http://www.infoworld.com/article/07/03/27/HNpersonalizedthre ats_1.html

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer